IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

Ari Givony, *individually and on behalf of all others similarly situated*, Plaintiff, v. University of Michigan and the Regents of the University of Michigan, Defendant.	Case No.: 5:23-cv-12783 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff Ari Givony ("Plaintiff") brings this Class Action Complaint against the University of Michigan and the Board of Regents of the University of Michigan (collectively "Defendants"), in her individual capacity and on behalf of all others similarly situated (the "Class" or "Class Members"), and alleges, upon personal knowledge as to her own actions and her counsels' investigations, and upon information and belief as to all other matters, as set forth herein:

INTRODUTION

1. This Class Action Complaint (the "Complaint") arises out of the recent targeted cyberattack and subsequent data breach spanning multiple days—from August 23 to 27, 2023 (the "Data Breach") on Defendant's network that resulted in unauthorized access of its students, applicants alumni, donors, employees, contractors, research study participants and patients s' sensitive personal data.

2. As a result of the Data Breach, Plaintiff and Class Members had their most sensitive personal information accessed, exfiltrated, and stolen, causing them to suffer ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack and Data Breach.

3. Information compromised in the Data Breach includes individuals' Social Security Numbers, driver's license or other government-issued ID number, financial account or payment card number, health information, payment card number, health insurance information, University Health Service and School of Dentistry clinical information, including patient medical numbers or diagnosis or treatment or medication history, and/or information related to participation in certain research studies (collectively, the "Private Information").

4. Majority of this information is protected information as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPPA").

5. Plaintiff brings this Class Action lawsuit in her individual capacity and on behalf of those similarly situated to address Defendant's inadequate safeguarding of Plaintiff's and Class Members' Private Information that it collected and maintained.

6. Defendant maintained the Private Information in a reckless and negligent manner. In particular, the Private Information was maintained on

Defendant's computer system and network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

7. Plaintiff's and Class Members' identities are at current and future risk because of Defendant's negligent conduct because the Private Information that Defendant collected and maintained was exposed and is now in the hands of data thieves and/or cyber criminals..

8. Armed with the Private Information accessed in the Data Breach, data thieves and cyber criminals can commit a variety of crimes including, but not limited to, opening new financial accounts in Class Members' names, applying for or taking out loans in Class Members' names, using Class Members' names to obtain medical services or benefits, using Class Members' Private Information to target other phishing and hacking intrusions based on their individual health needs, obtaining driver's licenses, passports or other forms of governmental-issued identification in Class Members' names but with another person's photograph and/or address, and giving false information to police during an arrest or detainment.

9. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of financial and medical fraud and identity theft. Plaintiff and Class Members must now and in the foreseeable future closely monitor their financial and healthcare accounts to guard against instances of fraud and identity theft.

10. Plaintiff and Class Members are likely to incur out of pocket costs for preventative and protective measures in order to deter or detect instances of fraud or identity theft, including purchasing credit monitoring services, purchasing and instilling credit freezes, purchasing and reviewing credit reports, or other protective measures as a direct cause of Defendants negligence.

11. By this Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the cyberattack and Data Breach.

12. Plaintiff seeks remedies including, but not limited to, compensatory damages, statutory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

13. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful and negligent conduct, and asserts the claims alleged below.

PARTIES

A. *Plaintiff Ari Givony*

14. Plaintiff Ari Givony is currently a resident and citizen of Plantation, Florida located in Broward County. Although the Data Brach occurred over multiple days in August 2023, Plaintiff did not receive notice of the Data Breach from Defendant until on or about October 23, 2023 (the "Notice").

15. The Notice further informed Plaintiff that the information potentially involved included Plaintiff and Class Members' Private Information, as the term is defined in paragraph 2.

16. Upon information and belief, Defendant currently and will continue to maintain copies of Plaintiff's and Class Members' Private Information on its computer systems and networks.

B. *Defendant University of Michigan*

17. Defendant the University of Michigan is a public research University located in Washtenaw County in Ann Arbor, Michigan that was founded in 1817 with its mailing address as 500 S. State Street, Ann Arbor, Michigan 48109.

18. Defendant advertises that it has over 32,000 undergraduate students enrolled in the current school year.

19. Upon information and belief, Defendant also employes approximately 35,000 employees.

C. *Defendant The Regents of the University of Michigan*

20. Defendant The Regents of the University of Michigan is a constitutional office of the State of Michigan and forms the governing body of the University of Michigan, which encompasses three (3) distinct campuses at Ann Arbor, Flint and Dearborn, all of which were compromised in the Data Breach.

21. Upon information and belief, the Board of Regents of the University of Michigan is currently comprised of eight (8) regents and includes Santa Ono, Michael J. Behm, Mark Bernstein, Sarah Hubbard, Denise Ilitch, Jordan Acker, Paul Brown, Ronald Weiser, and Katherine White.

JURISDICTION AND VENUE

22. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, upon information and belief there are more than 100 members in the proposed Class, and the Plaintiff is a citizen of a state different from Defendant to establish minimal diversity.

23. This District has personal jurisdiction over Defendant because Defendant and/or its parents or affiliates is headquartered in Michigan and many of the Class Members live outside of Michigan. Defendant conducts substantial business in Michigan. Defendant caused injury to Plaintiff in Texas.

24. Venue is proper in this District pursuant 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

ALLEGATIONS

D. *Defendant's Operations as a University*

25. Defendant is one of the nation's premier public higher education institutions. It was founded over a decade before Michigan was even recognized as a State.

26. On information and belief, in the ordinary course of business and as a condition of service, Defendant required patients, students, alumni, donors, applicants, contractors and employees, including Plaintiff, to provide copious amounts of sensitive personal and Private Information, such as the Private Information compromised in the Data Breach.

27. Upon information and belief, Defendant's Privacy Policy does not permit Defendant to disclose Plaintiff's and Class Members' Private Information for any reason via the Data Breach. In other words, the disclosure of Plaintiff's and Class Members' Private Information via the Data Breach was impermissible per Defendant's Privacy Policy.

28. Defendant's privacy policy provides that it limits "who has access to the personal information in our possession to only those who need it for a legitimate, specific purpose" and to "[p]rotect personal information through appropriate physical and technical security measures tailored to the sensitivity of the personal data [it] hold[s]."[1]

29. By obtaining, collecting, using, and deriving a benefit from Plaintiff and Class Members' Private Information, Defendant assumed legal and equitable duties and knew, or should have known, that it was responsible for protecting Plaintiff and Class Members' Private Information from unauthorized disclosure, exfiltration or access.

30. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

31. Plaintiff and the Class Members relied on and expected Defendant to keep their Private Information confidential and securely maintained, to use this information for business and health purposes only, and to make only authorized disclosures of this information to approved third-parties.

[1] https://umich.edu/about/privacy-statement/ (last visited: Nov. 1, 2023).

E. *The Cyberattack & Data Breach*

32. Over a span of four (4) days – between August 23 and August 27, 2023 – Defendant learned that it experienced a network security incident that involved an unauthorized party gaining access to Defendant's network environment and computer systemst. Upon detecting the incident, Defendant engaged a specialized third-party forensic incident response firm to assist with securing the network environment and investigating the extent of the Private Information compromised by the unauthorized activity. The investigation determined that the unauthorized third-party obtained the Private Information as a result.

33. Defendant notified Plaintiff and Class Members of the Data Breach on or about October 23, 2023.

34. When Defendant notified Plaintiff and Class Members, it failed to identify how many individuals were affected, when it discovered the full extent of the Data Breach, and precisely identify what information was compromised.

35. Upon information and belief, the Data Breach affected approximately 230,000 individuals.

36. Defendant has offered Plaintiff and Class Members twelve (12) months of complimentary credit monitoring services as a result of the Data Breach.

37. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant

would comply with its obligations to keep such information confidential and secure from unauthorized access, exfiltration or disclosure.

F. *Defendant Knew the Private Information on its Network was a Target*

38. In light of a number of recent high-profile data breaches at other educational institutions and companies in the healthcare industry, Defendant knew or should have known that their electronic records would be targeted by cybercriminals and data thieves.

39. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[2]

40. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[3]

[2] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited June 23, 2021).

[3] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited Aug. 24, 2021).

41. Therefore, the increase in such attacks, and attendant risk of future and ongoing attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

G. *Defendant Knew or Should Have Known of the Risk Because Companies in Possession of Private Information are Particularly Susceptible to Cyber Attacks.*

42. Data thieves and cyber criminals regularly target institutions like Defendant's due to the highly sensitive nature that it custodies records and data. Defendant knew and understood that unsecured and unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize the Private Information.

43. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.

44. According to cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyber attacks in 2019 alone.[4]

H. *Defendant Fails to Comply with FTC Guidelines*

45. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable

[4] *See* Maria Henriquez, Iowa City Hospital Suffers Phishing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attach (last visited on October 18, 2023).

data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

46. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

47. The FTC further recommends that companies not maintain Personally Identifiable Information ("PII") longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested and approved methods for security; routinely monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

48. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

49. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.")

50. Defendant failed to properly implement and maintain reasonable basic data security practices.

51. Defendant's failure to employ reasonable and appropriate measures to protect against and detect unauthorized third-party access to students, applicants alumni, donors, employees, contractors, research study participants and patients' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

52. Defendant was at all times fully aware of its obligation to protect the Private Information of students, applicants alumni, donors, employees, contractors, research study participants and patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

I. *Defendant Failed to Comply with Industry Standards*

53. Defendant failed to properly implement and maintain basic data security practices.

54. Defendant was at all times fully-aware of its obligation to protect the Private Information of its students, applicants alumni, donors, employees, contractors, research study participants and patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

55. Several best practices have been identified that at a minimum should be implemented by educational institutions and healthcare providers like Defendant, including, but not limited to: educating all employees; requiring strong passwords; using multi-layer security software, including firewalls, anti-virus, and anti-malware software; requiring encryption of data, making data unreadable without a key; requiring multi-factor authentication; creating and maintaining backup data, and; limiting which employees who can access sensitive data or Private Information.

56. Other best cybersecurity practices that are standard in the educational sector and healthcare industry include installing appropriate malware detection

software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

57. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

58. These foregoing frameworks are existing and applicable industry standards in the education and healthcare industries, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the Data Breach.

J. *Defendant's Conduct Violates HIPAA and Evidences Its Insufficient Data Security*

59. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive Private Information

60. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

61. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling Private Information like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

62. A Data Breach such as the one Defendant experienced, is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." *See* 45 C.F.R. 164.40

63. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

K. *Defendant's Breach*

64. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect students, applicants alumni, donors, employees, contractors, research study participants and patients Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to train its employees in the proper handling of emails containing Private Information and maintain adequate email security practices;

f. Failing to ensure the confidentiality and integrity of electronic Private Information it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic Private Information to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

h. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

j. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

k. Failing to protect against reasonably anticipated uses or disclosures of electronic Private Information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

l. Failing to ensure compliance with HIPAA security standard rules by its workforces in violation of 45 C.F.R. § 164.306(a)(4);

m. Failing to train all members of its workforces effectively on the policies and procedures regarding Private Information as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of Private Information, in violation of 45 C.F.R. § 164.530(b);

n. Failing to render the electronic Private Information it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic Private Information as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 CFR § 164.304's definition of "encryption"); and

o. Failing to adhere to industry standards for cybersecurity.

65. Defendant negligently and unlawfully failed to safeguard Plaintiff and Class Members' Private Information by allowing cyber criminals and data thieves to access Defendant's computer network and systems which retained unsecured and unencrypted Private Information.

66. Accordingly, as outlined below, Plaintiff and Class Members now face a present and substantially increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendant.

L. *Cyberattacks and Data Breaches Cause Disruption and Put Consumers at a Present and Substantially Increased Risk of Fraud and Identity Theft*

63. Cyberattacks and data breaches at educational institutions and healthcare providers like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

64. Researchers have found that among medical service providers that experience a data security incident, the death rate among patients increased in the months and years after the attack.[5]

65. Researchers have further found that at medical service providers that experienced a data security incident, the incident was associated with deterioration in timeliness and a decline in positive patient outcomes, generally.[6]

---

[5] *See* Nsikan Akpan, *Ransomware and Data Breaches Linked to Uptick in Fatal Heart Attacks*, PBS (Oct. 24, 2019), https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks (last visited Aug. 24, 2021).

[6] *See* Sung J. Choi et al., *Data Breach Remediation Efforts and Their Implications for Hospital Quality*, 54 Health Services Research 971, 971-980 (2019). Available at https://onlinelibrary.wiley.com/doi/full/10.1111/1475-6773.13203 (last visited Aug. 25, 2021).

66. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[7]

67. That is because any victim of a data breach is exposed to detrimental ramifications regardless of the nature of the data that was compromised. Indeed, the reason criminals steal Private Information is to monetize it. Particularly, cyber criminals and data thieves do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal or fraudulent financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate and correct pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security Number. Social engineering is a form of hacking whereby a data thief uses

[7] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007). Available at https://www.gao.gov/new.items/d07737.pdf (last visited Aug. 25, 2021).

previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam telemarking phone calls, text messages or phishing emails.

68. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the three (3) credit bureaus to place a fraud alert on their credit report and should consider filing an extended fraud alert that lasts for 7 years at a minimum unless you request to have it lifted before the 7 year period, which also takes substantial time and effort, in the event someone steals their identity, reviewing their credit reports, contacting companies or financial institutions to remove fraudulent charges from their accounts, placing a credit freeze on any lines of credit they currently have open, and correcting or amending their credit reports.[8]

69. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, telecommunication or utilities fraud, and banking or financial fraud.

70. Identity thieves can also use Social Security Numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government

[8] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/#/Steps (last visited Aug. 25, 2021).

benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

71. Moreover, theft of Private Information is also gravely serious. Private Information is an extremely valuable property right.[9]

72. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

73. Theft of health-related information (often referred to as PHI), in particular, is gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance

[9] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[10]

74. Pharmaceutical manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase Private Information on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves.

75. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and between when Private Information is stolen to when it is used for incidents of illegality or fraud and the damages become known.

76. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

[10] *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited Aug. 25, 2021).

77. Private Information is such a valuable commodity to cyber criminals and identity thieves that once the information has been compromised, criminals will often trade the information within in their possession with other cyber criminals and identitfy thieves on the "cyber black-market" for years.

78. There is a strong probability that entire batches of information stolen or exfiltrated from Defendant have already been or are yet bedumped on the black market, meaning Plaintiff and Class Members are at a present and substantially increased risk of fraud and identity theft for the foreseeable future.

79. Thus, Plaintiff and Class Members must vigilantly and proactively monitor and review their Private Information for many years to come.

80. Private Information can sell for as much as $363 per record according to the Infosec Institute.[11] Private Information is particularly valuable because criminals can use it to target victims with frauds and scams. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

81. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security Number to apply for new and

[11] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market,* InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Aug. 25, 2021).

additional credit lines.[12] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns or other tax related documents with the Internal Revenue Service, file for unemployment benefits, or apply for a job using a false identity.[13] Each of these fraudulent activities is difficult to detect. An individual may not know that their Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

82. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

83. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[14] Experian reports that a stolen credit or debit card

[12] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Aug. 25, 2021).

[13] *Id* at 4.

[14] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, *available at*:

number can sell for $5 to $110 on the dark web.[15] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[16]

84. Social Security Numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[17]

---

https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Oct. 27, 2021).

[15] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Oct. 27, 2021).

[16] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Oct. 27, 2021).

[17] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Oct. 27, 2021).

85. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[18]

86. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[19]

87. Medical information is especially valuable to identity thieves.

88. According to account monitoring company LogDog, the asking price for medical data is selling for $50 and up.[20]

---

[18] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Aug. 25, 2021).

[19] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Aug. 25, 2021).

[20] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019),

89. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

90. For this reason, Defendant knew or should have known about these dangers and strengthened its data and email handling systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet Defendant failed to properly prepare for that risk.

91. Based on the foregoing, the information compromised in this Data Breach is significantly more valuable than the loss of, for example, only credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach, includes Social Security Numbers, full legal names, and dates of birth, is impossible to "close" and difficult, if not impossible, to change.

92. Criminals are also able to piece together bits and pieces of compromised Private Information for develop what are called "Fullz" packages.[21]

---

https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last visited Aug. 25, 2021).

[21] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions

93. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

94. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

95. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the

---

over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/ (last visited on August 7, 2023).

unregulated data of Plaintiff and the other Class Members. Cybercriminals can then use this information to misrepresent their identity to gain access to financial and other accounts by providing verifying information compiled from unique sources.

96. Thus, even if certain information was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

97. To date, Defendant has done nothing to provide Plaintiff and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

98. Plaintiff's and Class Members' Private Information was compromised in the Data Breach and is now in the hands of the cybercriminals who accessed Defendant's computer systems and networks. Upon information and belief, these cybercriminals have published Plaintiff's and Class Members' Private Information to the internet and/or the "dark web".

99. Plaintiff's and Class Members' Private Information was compromised as a direct and proximate result of the Data Breach, which was a consequence of the inadequate and improper retention and data security practices used by Defendant at the time of the Data Breach

M. *Plaintiff Ari Givony's Experience.*

100. Plaintiff Givony provided his Private Information through an online form in order to participate in a research study.

101. As a condition to receiving services from the Defendant, Plaintiff provided her Private Information to Defendant, with the expectation that her Private Information would be safeguarded against cyberattacks and foreseeable theft and not disclosed for unauthorized purposes.

102. Although the Data Breach occurred in August 2023, Plaintiff did not receive Notice of the Data Breach from the Defendant until on or about October 23, 2023. The Defendant's Notice stated that her Private Information – as defined above – may have been accessed by an unauthorized third party.

103. The Data Breach has caused Plaintiff to suffer significant fear, anxiety, and stress. Plaintiff has lost sleep thinking about all the ways the Sensitive Information that was exposed can be used to commit various acts of fraud and identity theft.

104. Plaintiff suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Private Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

105. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her

Private Information being placed in the hands of unauthorized third parties and possibly criminals.

106. Plaintiff has a continuing interest in ensuring that Plaintiff's Private Information, which, upon information and belief, remain backed up in Defendant's possession, is protected, and safeguarded from future breaches.

N. *Plaintiff's and Class Members' Injuries and Damages*

107. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

108. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

109. Plaintiff and Class Members face the present and substantially increased risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

110. Plaintiff and Class Members face the present and substantially increased risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

111. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

112. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber criminals and data thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

113. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service or product that was intended to be accompanied by adequate data security but was not part of the price Plaintiff and Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of Defendant's computer systems and network and Plaintiff and Class Members' Private Information. Thus, Plaintiff and Class Members did not get what they paid for and agreed to.

114. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their medical accounts and Private Information for misuse.

115. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in

the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention or detection services;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and,

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

116. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage

of data or documents containing Private Information is not accessible online and that access to such data is password protected.

117. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

CLASS ACTION ALLEGATIONS

118. This action is properly maintainable as a class action. Plaintiff brings this class action on behalf of herself and all others similarly situated according to Rule 23 of the Federal Rules of Civil Procedure.

119. The Class that Plaintiff seeks to represent is defined as:

> All individuals and entities residing in the United States whose Private Information was compromised in the Data Breach that occurred approximately between August 23, 2023 to August 27, 2023.

120. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol

for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

121. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

122. **Numerosity:** The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. The Class is apparently identifiable within Defendant's records as the Notice letters indicate. It is believed that over 230,000 individuals are affected by this Data Breach.

123. **Commonality and Predominance:** Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiff and Class Members;

b. Whether Defendant had a duty not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had a duty not to use the Private Information of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members;

k. Whether Defendant was unjustly enriched by failing to properly protect Plaintiff's and Class Member's Private Information;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

124. **Typicality:** Plaintiff's claims are typical of those of the other members of the Class because Plaintiff, like every other member, was exposed to virtually identical conduct and now suffers from the same violations of the law as other members of the Class.

125. **Policies Generally Applicable to the Classes:** This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the proposed Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

126. **Adequacy:** Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief

that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

127. **Superiority and Manageability:** Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against a large corporation, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

128. Plaintiff and Class Members are ascertainable because Defendant's records will identify all victims and the subsequent data compromised in Defendant's Data Breach.

129. Plaintiff and Class Members are sufficiently numerous as to justify class certification. Specifically, the proposed Class exceeds forty (40) individuals.

130. Plaintiff and Class Members have a well-defined community of interest in pursuing relief from the harm that resulted from the Data Breach, including (1) predominant common questions of law or fact; (2) class representatives with claims or defenses typical of the class; and (3) a class representatives who can adequately represent the class.

131. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

132. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable

identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

133. Adequate notice can be given to Class Members directly using information maintained in Defendant's possession.

134. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

135. Although Defendant has offered to provide twelve (12) months of complimentary credit monitoring services to the Plaintiff and the Class, this is insufficient to repair the damage Defendant has caused, as alleged in this Complaint.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE AND NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and All Class Members)

136. Plaintiff and the Class repeat and reallege all foregoing paragraphs of this Complaint as if fully set forth herein.

137. As a condition of receiving services from Defendant, Defendant's current and former students, applicants alumni, donors, employees, contractors,

research study participants and patients' were obligated to provide Defendant with their Private Information.

138. Plaintiff and the Class entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would use reasonable measures to protect their Private Information and only make disclosures to third parties that are authorized.

139. Defendant has full knowledge of the sensitivity of the Private Information it held and maintained and the types of harm that Plaintiff and the Class could and would suffer if the Private Information were wrongfully disclosed.

140. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Private Information of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

141. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, exfiltrated, lost, stolen, misused, and/or otherwise disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant’s security protocols to ensure that the Private Information of Plaintiff and the Class in Defendant’s possession was adequately secured and protected.

142. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former students, applicants alumni, donors, employees, contractors, research study participants and patients Private Information that Defendant was no longer required to retain pursuant to regulations or legitimate business purposes.

143. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the Private Information of Plaintiff and the Class.

144. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant on the one hand and Plaintiff and the Class on the other. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential Private Information, a necessary part receiving services from Defendant. The special relationship also arose as a result of the nature of the relationship between Defendant and its students, applicants alumni, donors, employees, contractors, research study participants and patients' .

145. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

146. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable and preventable.

147. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and the Class, the critical importance of providing adequate security of that information, and the necessity for encrypting or redacting Private Information stored on Defendant's systems.

148. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions to not comply with industry standards for the safekeeping of the Private Information of Plaintiff and the Class, including basic encryption techniques freely available to Defendant.

149. Plaintiff and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

150. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

151. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff

and the Class to take steps to identify, prevent, mitigate, and repair any incident of identity theft and the fraudulent use of their Private Information by third-parties.

152. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the Private Information of Plaintiff and the Class.

153. Defendant has admitted that the Private Information of Plaintiff and the Class was accessed by cyber criminals or data thieves.

154. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the Private Information of Plaintiff and the Class during the time the Private Information was within Defendant's possession or control.

155. Defendant improperly and inadequately safeguarded the Private Information of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

156. Defendant failed to heed industry warnings, alerts and best practices to provide adequate safeguards to protect the Private Information of Plaintiff and the Class in the face of increased risk of theft.

157. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of its current and former students, applicants

alumni, donors, employees, contractors, research study participants and patients' Private Information.

158. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

159. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the Private Information of Plaintiff and the Class would not have been compromised.

160. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and the Class and the present harm, or risk of imminent harm, suffered by Plaintiff and the Class. The Private Information of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

161. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the

prevention, detection, mitigation and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of Plaintiff and the Class; and (viii) costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

162. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

163. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in

Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

164. Plaintiff and Class Members are therefore entitled to damages, including restitution and unjust enrichment, declaratory and injunctive relief, and attorneys' fees, costs, and expenses.

SECOND CAUSE OF ACTION
INVASION OF PRIVACY
(On Behalf of Plaintiff and All Class Members)

165. Plaintiff and the Class repeat and reallege all foregoing paragraphs as if fully set forth herein.

166. Plaintiff and the proposed Class had a legitimate expectation of privacy to their Private Information and were entitled to the protection of this information against disclosure to unauthorized third parties.

167. Defendant owed a duty to its current and former students, applicants alumni, donors, employees, contractors, research study participants and patients', including Plaintiff and the proposed Class, to keep their Private Information contained as a part thereof, confidential.

168. Defendant failed to protect and actually or potentially released to unknown and unauthorized third parties the Private Information of Plaintiff and the Class.

169. Defendant allowed unauthorized and unknown third parties to actually or potentially access and examine the Private Information of Plaintiff and the, by way of Defendant's failure to protect the Private Information. The unauthorized release to, custody of, and examination by unauthorized third parties of the Private Information of Plaintiff and the Class is highly offensive to a reasonable person.

170. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and the Class disclosed their Private Information to Defendant as part of Plaintiff's and the Class's relationships with Defendant, but privately with an intention that the Private Information would be kept confidential and would be protected from unauthorized disclosure.

171. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their explicit authorization.

172. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

173. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

174. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Class.

175. As a proximate result of the above acts and omissions of Defendant, the Private Information of Plaintiff and the Class was accessed by to third parties without authorization, causing Plaintiff and the Class to suffer damages.

176. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class in that the Private Information maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and the Class have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class.

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and All Class Members)

177. Plaintiff and the Class repeat and reallege all foregoing paragraphs as if fully set forth herein .

178. Defendant benefited from receiving Plaintiff's and Class Members' Private Information by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

179. Defendant also understood and appreciated that Plaintiff's and Class Members' Private Information was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

180. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of providing their Private Information to Defendant and Plaintiff's and Class Members' employers conferred a monetary benefit by purchasing loan services. In connection thereto, Plaintiff and Class Members and/or their employers provided Private Information to Defendant with the understanding that Defendant would pay for the administrative costs of reasonable data privacy and security practices and procedures. Specifically, Plaintiff and Class Members were required to provide their Private Information. In exchange, Plaintiff and Class Members should have received adequate protection and data security for such Private Information held by Defendant.

181. Defendant knew Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

182. Defendant failed to provide reasonable security, safeguards, and protections to the Private Information of Plaintiff and Class Members.

183. Under the principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Plaintiff and Class Members because

Defendant failed to implement appropriate data management and security measures mandated by industry standards.

184. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class Members.

185. Defendant's enrichment at the expense of Plaintiff and Class Members is and was unjust.

186. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff and the Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

FOURT CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and All Class Members)

187. Plaintiff and the Class repeat and reallege all foregoing paragraphs as if fully set forth herein.

188. Plaintiff and the Class Members delivered their Private Information to Defendant as part of the process of obtaining services provided by Defendant.

189. Plaintiff and Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members if and when their data had been breached and compromised. Each such contractual relationship

imposed on Defendant an implied covenant of good faith and fair dealing by which Defendant was required to perform its obligations and manage Plaintiff's and Class Members' data in a manner which comported with the reasonable expectations of privacy and protection attendant to entrusting such data to Defendant.

190. In providing their Private Information, Plaintiff and Class Members entered into an implied contract with Defendant whereby Defendant, in receiving such data, became obligated to reasonably safeguard Plaintiff's and the other Class Members' Private Information.

191. In delivering their Private Information to Defendant, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard that data.

192. Plaintiff and the Class Members would not have entrusted their Private Information to Defendant in the absence of such an implied contract.

193. Defendant accepted possession of Plaintiff's and Class Members' personal data for the purpose of providing medical services to Plaintiff and Class Members.

194. Had Defendant disclosed to Plaintiff and Class Members that Defendant did not have adequate computer systems and security practices to secure students, applicants alumni, donors, employees, contractors, research study

participants and patients' s' Private Information, Plaintiff and members of the Class would not have provided their Private Information to Defendant.

195. Defendant recognized that its current and former students, applicants alumni, donors, employees, contractors, research study participants and patients s' Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and Class Members.

196. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

197. Defendant breached the implied contract with Plaintiff and Class Members by failing to take reasonable measures to safeguard their data.

198. Defendant breached the implied contract with Plaintiff and Class Members by failing to promptly notify them of the access to and exfiltration of their Private Information.

199. As a direct and proximate result of the breach of the contractual duties, Plaintiff and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiff and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and Class Members' Private Information; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e)

economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their Private Information; (g) the diminution in the value of the services bargained for as Plaintiff and Class Members were deprived of the data protection and security that Defendant promised when Plaintiff and the proposed class entrusted Defendant with their Private Information; and (h) the continued and substantial risk to Plaintiff and Class Members Private Information, which remains in the Defendant's possession of Defendant with inadequate measures to protect Plaintiff's and Class Members' Private Information.

FIFTH CAUSE OF ACTION
BREACH OF EXPRESS CONTRACT
(On Behalf of Plaintiff and All Class Members)

200. Plaintiff and the Class repeat and reallege all foregoing paragraphs.

201. Plaintiff and Class Members entered into valid and enforceable contracts through which they were required to turn over their Private Information to Defendant in exchange for services, employment, or admittance. Those contracts included promises that Defendant would safeguard, secure, and not disclose Plaintiff and Class Members' Private Information to any third parties without Plaintiff or Class Members' consent.

202. Defendant's privacy statement memorialized the rights and obligations of the Defendant to Plaintiff and the Class. The Defendant's privacy statement became part of the agreement Plaintiff and Class had with Defendant for services.

203. Defendant's privacy statement promised Plaintiff and the Class to protect the privacy and security of their Private Information and never to share Plaintiff or Class Members' Private Information without their consent, or under limited circumstances.

204. Plaintiff and Class Members fully performed their obligations under their agreements with Defendant. But, Defendant failed to secure, safeguard, and/or keep Plaintiff and Class Members' Private information private. Accordingly, Defendant breached its agreements with Plaintiff and Class.

205. As a direct and proximate result of the breach of the contractual duties, Plaintiff and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiff and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and Class Members' Private Information; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing

related to the theft and compromise of their Private Information; (g) the diminution in the value of the services bargained for as Plaintiff and Class Members were deprived of the data protection and security that Defendant promised when Plaintiff and the proposed class entrusted Defendant with their Private Information; and (h) the continued and substantial risk to Plaintiff and Class Members Private Information, which remains in the Defendant's possession of Defendant with inadequate measures to protect Plaintiff's and Class Members' Private Information.

SIXTH CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and All Class Members)

206. Plaintiff and the Class repeat and reallege all foregoing paragraphs as if fully set forth herein.

207. Plaintiff and Class Members gave Defendant their Private Information in confidence, believing that Defendant would protect that information. Plaintiff and Class Members would not have provided Defendant with this information had they known it would not be adequately protected. Defendant's acceptance and storage of Plaintiff's and Class Members' Private Information created a fiduciary relationship between Defendant and the Plaintiff and Class Members. In light of this relationship, Defendant must act primarily for the benefit of the Plaintiff and the Class Members, which includes taking appropriate steps to safeguard and protect their Private Information.

208. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their relationship.

209. Defendant breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class Members' Private Information, failing to comply with the applicable data security laws, standards, and guidelines, and otherwise failing to safeguard Plaintiff's and Class Members' Private Information that it collected.

210. As a direct and proximate result of the breach of the contractual duties, Plaintiff and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiff and the Class Members include: (a) the invasion of privacy; (b) the compromise, exfiltration, disclosure, theft, and unauthorized use of Plaintiff's and Class Members' Private Information; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their Private Information; (g) the diminution in the value of the services bargained for as Plaintiff and Class Members were deprived of the data protection and security that Defendant promised when Plaintiff and the proposed class entrusted Defendant with their Private Information; and (h)

the continued and substantial risk to Plaintiff and Class Members Private Information, which remains in the Defendant's possession of Defendant with inadequate measures to protect Plaintiff's and Class Members' Private Information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an order certifying the Class, as defined herein, and appointing Plaintiff and her Counsel to represent each such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database or server;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering

Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal Private Information and other relevant data;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential Private Information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment and/or post-judgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Respectfully Submitted,

Dated: November 1, 2023

/s/Philip J. Krzeski

Bryan L. Bleichner (CAL BAR # 220340)
Philip J. Krzeski (MN BAR #0403291)
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Telephone: (612) 339-7300
bbleichner@chesnutcambronne.com
pkrzeski@chestnutcambronne.com

Joseph M. Lyon (OH BAR #0076050)
THE LYON LAW FIRM, LLC
2754 Erie Avenue
Cincinnati, OH 45208
Telephone: (513) 381-2333
Facsimile: (513) 766-9011
jlyon@thelyonfirm.com

Attorneys for Plaintiff and the Proposed Class